UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

CASE NO. 13-CR-136 (MJD/TNL)

UNITED STATES OF AMERICA,

Plaintiff,

v. **REPORT & RECOMMENDATION**

GUY EDWARD WHEELOCK,

Defendant.

Manda M. Sertich, Assistant United States Attorney, **UNITED STATES ATTORNEY'S OFFICE**, 300 South Fourth Street, Suite 600, Minneapolis, MN 55415, for the Government; and

Alan D. Margoles, **MARGOLES & MARGOLES**, 790 Cleveland Avenue South, Suite 223, St. Paul, MN 55116, for Defendant.

This matter is before the Court, Magistrate Judge Tony N. Leung, on Defendant Guy Edward Wheelock's Motion to Dismiss for Lack of Jurisdiction (ECF No. 19) and Wheelock's Motions to Suppress Evidence (ECF Nos. 23, 28, 31). Defendant is charged with possession, receipt and attempted distribution of child pornography in violation of 18 U.S.C. §§ 2552(a)(2), (a)(4)(B), (b)(1) and (b)(2).

The Court heard oral argument on Defendant's motions. Alan D. Margoles represented Defendant, and Manda M. Sertich represented the United States of America. The Court heard testimony from Officer Dale Hanson of the Minneapolis Police Department. The Court received the following exhibits: Government Exhibit 1A is a Request for Administrate Subpoena dated September 3, 2011 and signed by Officer

Hanson; Government Exhibit 1B is an Administrative Subpoena issued from the Hennepin County Attorney's office and dated September 7, 2011; Government Exhibit 1C is Comcast's written response to the September 7, 2011 Administrative Subpoena; Government Exhibit 2A is a Request for Administrate Subpoena dated September 25, 2011 and signed by Officer Hanson; Government Exhibit 2B is an Administrative Subpoena issued from the Hennepin County Attorney's office and dated September 26, 2011; Government Exhibit 2C is Comcast's written response to the September 26, 2011 Administrative Subpoena; Government Exhibit 3A is a Request for Administrate Subpoena dated October 24, 2011, signed by Officer Hanson; Government Exhibit 3B is an Administrative Subpoena issued from the Hennepin County Attorney's office dated October 24, 2011; Government Exhibit 3C is Comcast's written response to the October 24, 2011 Administrative Subpoena; Government Exhibit 4A is a Request for Administrate Subpoena dated January 10, 2012, signed by Officer Hanson; Government Exhibit 4B is an Administrative Subpoena issued from the Hennepin County Attorney's office dated January 10, 2012; Government Exhibit 4C is Comcast's written response to the January 10, 2012 Administrative Subpoena; and Government Exhibit 5 is a search warrant and supporting affidavit dated February 1, 2012, signed by Officer Hanson and Anoka County District Judge John P. Dehen.

I. FACTS

Officer Hanson is employed by the Minneapolis Police Department and a member of the Minnesota Internet Crimes Against Children Task Force and the FBI's Child Exploitation Task Force. (Tr. 13.) In 2011, Officer Hanson was informed while using

investigative software that child pornography files were available from the Internet Protocol ("IP") address 76.113.242.167 assigned on August 26, 2011, at 8:34 a.m. (Tr. 15; Gov't Ex. 1-A.) On September 3, 2011, Officer Hanson submitted a request to the Hennepin County Attorney's Office for an administrative subpoena pursuant to Minn. Stat. § 388.23. (Gov't Ex. 1-A.) This request sought all subscriber information, IP address history, email addresses and billing information associated with IP address 76.113.242.167 assigned on August 26, 2011, at 8:34 a.m. from Comcast Communications ("Comcast"), the relevant Internet service provider ("ISP"). (*Id.*) In the request, Officer Hanson certified "that the requested records are relevant to an ongoing, legitimate law enforcement investigation of Distribution of Child Pornography." (*Id.*)

On September 7, 2011, the Hennepin County Attorney's Office faxed Comcast an administrative subpoena for the requested information. (Gov't Ex. 1-B.) Comcast responded to the administrative subpoena on September 8, 2011. (Gov't Ex. 1-C.) The response indicated that the Comcast subscriber associated with the specified IP address on August 26, 2011, at 8:34 a.m. was Defendant. (*Id.*) Comcast's response also provided Officer Hanson with Defendant's name and physical address. (Tr. 38-39.) Officer Hanson checked the Minnesota sex offender registry and discovered that Defendant was a Level 1 sex offender with a previous conviction for possession of child pornography. (Tr. 39.) The sex offender registry also listed Defendant's address. (Tr. 39.)

Officer Hanson submitted three more administrative subpoena requests to the Hennepin County Attorney's Office concerning IP address 76.113.242.167. (Gov't Exs. 2-A, 3-A, 4-A.) The Hennepin County Attorney's Office issued administrative subpoenas

to Comcast pursuant to Officer Hanson's requests (Gov't Exs. 2-B, 3-B, 4-B), and Comcast's responses to the subpoenas indicated that the Comcast subscriber associated with the specified IP address was Defendant. (Gov't Exs. 2-C, 3-C, 4-C.) Using the information obtained from the administrative subpoenas, Officer Hanson obtained a search warrant for Defendant's house. (Gov't Ex. 5.)

On February 2, 2012, Officer Hanson and several other officers executed the search warrant at Defendant's residence. (Tr. 22-23.) During the search, officers discovered a computer downloading child pornography video files using Shareaza, a peer-to-peer file-sharing program. (Tr. 23-24.) Officers seized the computer, as well as several hard drives, CDs and DVDs. (Tr. 25.) A subsequent forensic examination of the items seized during the search revealed the presence of a number of child pornography files. (Tr. 25.) Officer Hanson testified that, according to information he received from the National Center for Missing and Exploited Children ("NCMEC"), none of the files for which Defendant has been indicted were produced inside Minnesota. (Tr. 26-27.) Officer Hanson also testified that, although he had not specifically investigated the manufacturer of each digital media item seized from Defendant's home, it is "very possible" that the CDs and DVDs were manufactured outside of Minnesota. (Tr. 27-28.)

II. ANALYSIS

A. Motion to Dismiss for Lack of Jurisdiction

Defendant has moved to dismiss the indictment for lack of jurisdiction, arguing that (a) the Government has not provided sufficient evidence that Defendant distributed illegal child pornography in interstate commerce and across state lines, and (2) the

Government has not provided sufficient evidence that the individual items of child pornography for which Defendant was indicted were obtained through interstate commerce and traveled across state lines. (ECF No. 19.)

When considering a pretrial motion to dismiss an indictment, the allegations contained in the indictment should be accepted as true. *See United States v. Najarian*, 915 F. Supp. 1460, 1463 n.3 (D. Minn. 1996) (citing *inter alia, United States v. Sampson*, 371 U.S. 75, 78-79 (1962)). "[F]ederal criminal procedure does not 'provide for a pre-trial determination of sufficiency of the evidence.'" *United States v. Ferro*, 252 F.3d 964, 968 (8th Cir. 2001) (quoting *United States v. Critzer*, 951 F.2d 306, 307-08 (11th Cir. 1992)). "Indictments are normally sufficient unless no reasonable construction can be said to charge the offense." *United States v. Nabors*, 45 F.3d 238, 240 (8th Cir. 1995) (citation omitted).

Defendant challenges the interstate nexus underlying the counts in the indictment. The Court finds this challenge unpersuasive. "[T]he government may satisfy the interstate commerce element by proving that child pornography images [or video] w[as] transmitted over the Internet." *United States v. Lewis*, 554 F.3d 208, 215 (1st Cir. 2009) (citation omitted); *see also United States v. MacEwan*, 445 F.3d 237, 244 (3d Cir. 2006) ("because of the very interstate nature of the Internet, once a user submits a connection request to a website server or an image is transmitted from the website server back to the user, the data has traveled in interstate commerce."); *United States v. Runyan*, 290 F.3d 223, 239 (5th Cir.) ("[T]ransmission of photographs by means of the Internet is tantamount to moving photographs across state lines and thus constitutes transportation in

interstate commerce."), *cert. denied*, 537 U.S. 888 (2002); *United States v. Whiting*, 165 F.3d 631, 634 (8th Cir. 1999) (noting that the defendant had "downloaded images from the Internet through interstate commerce using a computer"); Manual of Model Criminal Jury Instructions for the Eighth Circuit § 6.16.2252A(2) at 384 (2007) ("Images transmitted or received over the Internet have moved in interstate or foreign commerce.") (citations omitted); *see generally, United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (per curiam) (quoting *MacEwan*, 445 F.3d at 245) ("As both the means to engage in commerce and the method by which transactions occur, 'the Internet is an instrumentality and channel of interstate commerce.' With a connection to the Internet, the Salvation Army's computers were part of 'a system that is inexorably intertwined with interstate commerce' and thus properly within the realm of Congress's Commerce Clause power.").

Counts 1-7 of the indictment charge Defendant with attempted distribution of child pornography under 18 U.S.C. §§ 2252(a)(2) and (b)(1). Officer Hanson testified at the motions hearing that investigative software he employed informed him that child pornography files were available for download from Defendant's IP address on the Internet via a peer-to-peer file sharing service. Accordingly, the Court determines that the Government met the interstate-nexus requirement.

Count 8 charges Defendant with receipt of child pornography. The Government put forth evidence and testimony that Defendant was downloading child pornography videos from the Internet while officers were executing the search warrant. Because the videos were being transmitted over the Internet, they were moving through interstate

commerce. *See United States v. Patton*, No. 09-cr-43 (PAM/JSM), 2009 WL 1514502, at *2 (D. Minn. June 1, 2009). Accordingly, the interstate nexus requirement has been met for Count 8.

Count 9 of the indictment charges Defendant with knowing possession of child pornography that was "transported in interstate or foreign commerce by any means." *United States v. White*, 506 F.3d 635, 641 (8th Cir. 2007). The Government put forth evidence that the videos found on the media seized during the search of Defendant's home were produced outside the state of Minnesota. Officer Hanson also testified that it was very possible that the CDs and DVDs containing child pornography were manufactured outside of Minnesota. *See United States v. Inman*, 558 F.3d 742, 751 (8th Cir. 2009) (noting that evidence that the defendant's hard drive and DVDs traveled in interstate or foreign commerce was sufficient to meet the jurisdictional element of a possession of child pornography charge). Accordingly, the interstate nexus requirement for Count 9 has been met.

Accepting all the allegations in the indictment as true, the Government has satisfied the interstate nexus requirement of Counts 1-9. Accordingly, Defendant's motion to dismiss for lack of jurisdiction must be denied.

B. Motions to Suppress Evidence

Defendant also moves to suppress all evidence obtained in the search of his home, arguing that Officer Hanson's use of the Minnesota administrative subpoena process to discover his name and address violated Defendant's Fourth Amendment rights, the

federal administrative subpoena statute, 18 U.S.C. § 3486, and the Minnesota administrative subpoena statute, Minn. Stat. § 388.23.

1. Fourth Amendment Challenge

Defendant argues that Officer Hanson's use of administrative subpoenas violated his expectation of privacy in the personally identifiable information he gave Comcast. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures."

> An individual may challenge a search under the Fourth Amendment if it violates the individual's "reasonable expectation of privacy," *United States v. Jones*, 132 S. Ct. 945, 950-53 (2012) (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)), or involves an unreasonable "physical intrusion of a constitutionally protected area," *id.* (quoting *United States v. Knotts*, 460 U.S. 276, 286 (1983) (Brennan, J., concurring in the judgment) (internal quotation marks omitted)) in order to find or obtain some information.

United States v. Cowan, 674 F.3d 947, 955 (8th Cir. 2012). To be successful in his challenge, Defendant must show that he had a subjective expectation of privacy in the areas searched that society is prepared to accept as objectively reasonable. *E.g.*, *United States v. James*, 534 F.3d 868, 872 (8th Cir. 2008).

a. Defendant Has No Reasonable Expectation of Privacy in the Personally Identifiable Information He Gave Comcast

It is well established that there is no reasonable expectation of privacy where an individual discloses information to a third party, even where that information is understood to be confidential. *See Katz*, 389 U.S. at 363 (White, J., concurring) ("When one man speaks to another, he takes all the risks ordinarily inherent in doing so, including

the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable (or law-abiding) associates."); *Smith v. Maryland*, 442 U.S. 735 (1979) (finding no objectively reasonable expectation of privacy in dialed telephone numbers). This third-party disclosure doctrine applies in cases of warrantless searches as well as administrative subpoenas. *S.E.C. v. Jerry T. O'Brien*, 467 U.S. 735, 743 (1984).

Defendant made the conscious choices to share (1) the files in question over a peer-to-peer network on the Internet, and (2) his name and address with his ISP. These choices divested Defendant of any expectation of privacy in the government's acquisition of his subscriber information, including his name, billing address, and IP address from his ISP. *United States v. Stults*, 575 F.3d 834, 842 (8th Cir. 2009) (citing *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (holding that defendant had no expectation of privacy in his subscriber information, including his IP address and name from third-party service providers, where the defendant voluntarily provided such information to his ISP and enabled peer-to-peer file sharing on his computer)).

Defendant argues that Minnesota's Internet Privacy Act creates an objectively reasonable expectation of privacy in the identifying information he provided to his ISP. The Internet Privacy Act provides that an ISP may not knowingly disclose a consumer's "personally identifiable information." Minn. Stat. § 325M.02. The statute defines "personally identifiable information" as information that identifies:

> (1) a consumer by physical or electronic address or telephone number;
> (2) a consumer as having requested or obtained specific materials or services from an Internet service provider;

(3) Internet or online sites visited by a consumer; or
(4) any of the contents of a consumer's data-storage devices.

Id. § 325M.01, subd. 5. The Internet Privacy Act contains an exception that requires ISPs to disclose personally identifiable information "pursuant to subpoena, including administrative subpoena, issued under authority of law of this state or another state or the United States." Minn. Stat. § 325M.03(6).

Here, Comcast provided information, including Defendant's name and physical address, to law enforcement pursuant to an administrative subpoena. Officer Hanson's administrative subpoena requested personally identifiable information as allowed by § 325M.03, and his request included a certification "that the requested records [were] relevant to an ongoing, legitimate law enforcement investigation of Distribution of Child Pornography," (Gov't Exs. 1-A, 2-A, 3-A, 4-A), as required my Minnesota law. *See* Minn. Stat. § 388.23. An assistant county attorney reviewed and signed each of the requests seeking specific information from Comcast, Defendant's ISP. (Gov't Exs. 1-B, 2-B, 3-B, 4-B.) The administrative subpoenas at issue were all issued under the laws of Minnesota, and therefore, § 325.03 *required* Comcast to provide the requested information. This disclosure requirement defeats any argument that the statute creates an expectation of privacy. Accordingly, the Court determines that Minnesota's Internet Privacy Statute does not create an objectively reasonable expectation of privacy in such information.

b. Defendant's Reliance on *United States v. Jones* is Unfounded

Defendant also argues that the concurring opinions[1] of five members of the Supreme Court in *United States v. Jones*, 132 S. Ct. 945 (2012), bolster his argument that § 325M creates an objectively reasonable expectation of privacy. *Jones*, however, is inapplicable to the instant case. There, the Court held that a physical trespass for the purpose of gathering information constitutes a Fourth Amendment search, *id.* at 952, but specifically avoided what effect its decision might have on "some future case where a classic trespassory search is not involved." *Id.* at 953. In doing so, the Court made clear that "the *Katz* reasonable-expectation test has been added to, not substituted for, the common-law trespassory test." *Id.* at 952.

Defendant relies on a statement in Justice Alito's concurring opinion that, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative," *id.* at 964, to argue that this Court should give great weight to an expectation of privacy created by Minn. Stat. § 325M. To argue that the third-party disclosure doctrine should not be followed in this case, Defendant also relies on a statement in Justice Sotomayor's concurring opinion that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," *id.* at 957.

[1] Defendant relies on Justice Sotomayor's concurring opinion, *United States v. Jones*, 132 S. Ct. 945, 954 (2012), and Justice Alito's opinion concurring in the judgment, *id.* at 957, which was joined by Justices Ginsburg, Breyer, and Kagan.

As set forth above, however, § 325M does not create an objectively reasonable expectation of privacy. The statute requires disclosure of personal identifying information in response to a subpoena. Such a requirement belies a determination that any expectation of privacy in the same information is objectively reasonable. More fundamentally, the concurring opinions of Justices Alito and Sotomayor are just that—concurring opinions. This Court reads *Jones* to stand for the proposition that a physical trespass for the purpose of gathering information constitutes a Fourth Amendment search and therefore requires a warrant. Whether the third-party disclosure doctrine or technology may someday change the "hypothetical reasonable person[']s] . . . well-developed and stable set of privacy expectations," *id*. at 962 (Alito, J., concurring in the judgment), is best left for "some future case where a classic trespassory search is not involved." *Id.* at 953.

Taking all the circumstances into account, Minnesota's Internet Privacy Act requires ISPs to disclose subscriber information pursuant to an administrative subpoena. Defendant cannot, therefore, prove a Fourth Amendment violation based on his ISP's disclosure of his personally identifying information pursuant to valid administrative subpoenas. Accordingly, Defendant "has failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable." *United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (citing *James*, 534 F.3d at 872).

2. Federal Administrative Subpoena Statute Does Not Apply to the Administrative Subpoenas in This Case

Defendant also argues that the administrative subpoenas used by Officer Hanson violated the Federal Administrative Subpoena Statute, 18 U.S.C. § 3486. This argument

is unfounded. The administrative subpoenas used in this case were issued pursuant to Minnesota law, not federal law. There is no basis for Defendant's argument that Minnesota's administrative subpoena processes should meet federal standards or satisfy federal statutory requirements. Accordingly, whether the administrative subpoenas satisfied the requirements of 18 U.S.C. § 3486 has no effect on the subpoenas' validity.

Even if the federal administrative subpoena statute applied, the administrative subpoenas here complied with all statutory requirements. A subpoena issued pursuant to § 3486(a)(1)(A) that is served upon an ISP may require that provider to disclose information "which may be relevant to an authorized law enforcement inquiry," including the subscriber's name and address, *id.* § 3486(a)(1)(C)(i). Moreover, Officer Hanson was not required to obtain an *ex parte* gag order because the section providing for *ex parte* gag orders is optional, not mandatory, *see id.* § 3486(a)(6)(A) ("A United States district court for the district in which the summons is or will be served, upon application of the United States, *may* issue an ex parte order that no person disclose to any other person . . . the existence of such summons for a period of up to 90 days.") (emphasis added). Accordingly, Defendant's challenge on that basis must be denied.

3. Administrative Subpoenas Satisfied Minnesota Statutory Requirements

Defendant also argues that the administrative subpoenas violated both Minnesota's Administrative Subpoena Statute, Minn. Stat. § 388.23, and Minnesota's Internet Privacy Act, Minn. Stat. § 325M. This argument fails for several reasons.

First, whether or not the administrative subpoenas used in this case violated Minnesota law, however, does not affect the admissibility of the fruits of the subpoenas. The Fourth Amendment is not a vehicle for enforcing state law. *See Virginia v. Moore*, 553 U.S. 164, 178 (2008) (refusing to find an arrest based on probable cause unreasonable even though the arrest was prohibited by state law); *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002) ("[F]ederal courts in a federal prosecution do not suppress evidence that is seized by state officers in violation of state law, so long as the search complied with the Fourth Amendment."); *United States v. Guthmiller*, No. 09-cr-258 (ADM/AJB), 2010 WL 55986, at *2 (D. Minn. Jan 4, 2010) (citing *Moore*, 553 U.S. 164). "[E]ven if Defendant had an expectation of privacy in subscriber information as a matter of state law," which this Court need not address, "he does not have a federal constitutional expectation of privacy in such information." *Guthmiller*, 2010 WL 55986, at *2.

Second, the Court determines that Minnesota law was not violated. As stated above, Minnesota's Internet Privacy Act not only allows but *requires* ISPs to disclose such information pursuant to a valid subpoena. Minn. Stat. § 325M.03, subd. 6. The Minnesota administrative subpoena statute provides, "[t]he county attorney . . . has the authority to subpoena and require the production of any records of . . . subscribers of private computer networks including Internet service providers . . . . that are relevant to an ongoing legitimate law enforcement investigation." *Id.* § 388.23, subd. 1. Contrary to Defendant's argument, Minnesota's administrative subpoena statute does not require the county attorney to review the substance of the request. *See. id.* Officer Hanson's

administrative subpoena requested personally identifiable information as allowed by § 325M.03, and his request included a certification "that the requested records [were] relevant to an ongoing, legitimate law enforcement investigation of Distribution of Child Pornography." (Gov't Exs. 1-A, 2-A, 3-A, 4-A.) An assistant county attorney reviewed and signed each of the requests seeking specific information from Comcast, Defendant's ISP. (Gov't Exs. 1-B, 2-B, 3-B, 4-B.) Neither the Internet Privacy Act nor the Administrative Subpoena Statute places any further burden on Officer Hanson or the Anoka County Attorney's Office. The Court determines that the administrative subpoenas in this case complied with the Minnesota law. Accordingly, Defendant's challenge that the subpoenas at issue violated Minnesota law must also fail.

4. Conclusion

Based on the foregoing, this Court determines that no Fourth Amendment violation resulted from Officer Hanson's use of administrative subpoenas or the information obtained from Comcast. Defendant's motions to suppress evidence must be denied.

III. RECOMMENDATION

Based on the foregoing and all the files, records and proceedings herein, **IT IS HEREBY RECOMMENDED** that Defendant Guy Edward Wheelock's Motion to Dismiss (ECF No. 19) and Motions to Suppress (ECF Nos. 23, 28, 31) be **DENIED**.

Date: September 13, 2013

s/ Tony N. Leung
Tony N. Leung
United States Magistrate Judge
District of Minnesota

United States v. Guy Edward Wheelock
File No. 13-cr-136 (MJD/TNL)

Pursuant to Local Rule 72.2(b), any party may object to this Report and Recommendation by filing with the Clerk of Court and by serving upon all parties written objections that specifically identify the portions of the Report to which objections are made and the basis of each objection. This Report and Recommendation does not constitute an order from the District Court and it is therefore not directly appealable to the Circuit Court of Appeals. Written objections must be filed with the Court before **September 30, 2013**.